

h

Notice of Allowability	Application No.	Applicant(s)	
	09/609,809	LOTSPIECH, JEFFREY BRUCE	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to phone conversation held on 4/7/2005 and amendment received by fax on 4/8/2005.
2. ☒ The allowed claim(s) is/are 6-12 and 15-17.
3. ☒ The drawings filed on 03 July 2000 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

TL

DETAILED ACTION

Reasons for Allowance

1. In response to the last phone conversation between the Examiner and Applicant's Representative, John Rogitz on 4/7/2005, a faxed amendment was received by the Office on 4/8/2005 in which some informalities were corrected in claims 8 and 12. Claim 6 was also amended to replace program storage device to readable medium to better direct the claimed invention to a statutory subject matter.

The following is an examiner's statement of reasons for allowance:

The prior art of record, 6,772,343 to Shimizu, teaches a data processor in which a plain text or a cipher text is segmented into two small blocks and the new small blocks are encrypted or decrypted. The data processor comprises means for transforming small blocks with keys and means for chaining small blocks. Applicant's argument filed on 1/27/2005 has been persuasive. As indicated by Applicant, Shimizu, teaches a scrambling and chaining process but fails to teach a scrambling result XORed with another plain text block in the iterating step as claimed in claim 6. The prior arts of record taken alone or in combination fail to teach, anticipate, suggest, or render obvious the claimed invention. Consequently, independent claim 6 is allowable over the prior art of record. Claim 7 is directly or indirectly dependent upon claim 6; therefore claim 7 is also allowable over the prior art of record.

Independent claim 8 describes a computer system for encrypting a stream of data blocks, and contains similar and more specific limitations than claim 6. Claim 8 also discloses determining whether a predetermined number of iterations has been executed if not returning to

the beginning of the loop using a next round of cipher otherwise outputting a next round of cipher. The prior arts of record taken alone or in combination fail to teach, anticipate, suggest, or render obvious the claimed invention. Consequently, independent claim 8 is allowable over the prior art of record. Claims 9 and 10 are directly or indirectly dependent upon claim 8; therefore claims 9 and 10 are also allowable over the prior art of record.

With respect to claim 11, the method of Shimizu as pointed by Applicant does not iterate through the rounds of cipher by iterating through respective outer loops of forward plaintext chaining followed by backward plaintext chaining while during each forward portion of an outer loop, applying a respective round of the cipher to each block. The prior arts of record taken alone or in combination fail to teach, anticipate, suggest, or render obvious the claimed invention. Consequently, independent claim 11 is allowable over the prior art of record. Claim 12 is directly or indirectly dependent upon claim 11; therefore claim 12 is allowable over the prior art of record.

Independent claim 15 recites a computer system for decrypting a stream of data blocks. Claim 15 discloses an inverse process of allowed claim 8. Consequently, claim 15 is allowable over the prior art of record. Claims 16 and 17 are directly or indirectly dependent upon claim 15; therefore claims 16 and 17 are allowable over the prior art of record.

2. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
April 14, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100